PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-157837
(43)Date of publication of application : 29.05.1992

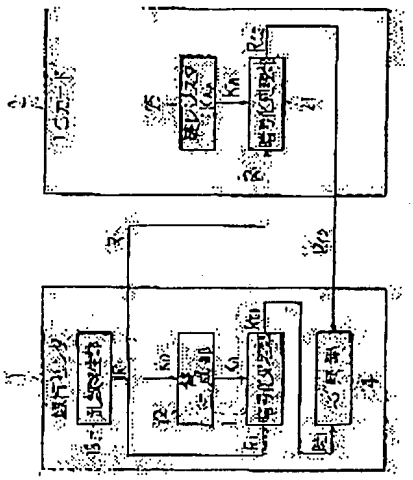
(51)Int.Cl. H04L 9/28
H04K 1/02

(21)Application number : 02-283195
(22)Date of filing : 20.10.1990

(71)Applicant : FUJITSU LTD
(72)Inventor : HASEBE TAKAYUKI
AKIYAMA RYOTA

(54) KEY SUPPLY SYSTEM FOR CIPHER PROCESSING

(57)Abstract:
PURPOSE: To apply cipher processing based upon a DES system even to a device whose storage means quantity is limited by providing a an IC card with a key register as a key storage means.
CONSTITUTION: A bank center 1 is provided with a encipherment processing part 11, a key generation part 12, a random number generation part 13, and a comparison part 14, but the IC card 2 is provided with the key register 25 instead of the key generation part 23. The random number generation part 13 provided in the bank center 1 generates and inputs a random number R1 to the encipherment processing part 11, and also transfers the random number even to the IC card 2, so that it is inputted to its encipherment part 21. The encipherment processing parts 11 and 21 convert the input random number R1 into enciphered random numbers RC1 and RC2, which are sent to the comparison part 14 provided in the bank center 1 and compared with each other, so that the bank center 1 authenticates the IC card 2 when both the random number are equal to each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－157837

⑤1Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成4年(1992)5月29日
H 04 L 9/28			
H 04 K 1/02		7117－5K	
		7117－5K　H 04 L 9/02	A

審査請求　未請求　請求項の数　6　（全15頁）

⑤4発明の名称　暗号処理用鍵供給方式

⑳特　願　平2－283195

㉒出　願　平2(1990)10月20日

⑦2発明者　長谷部　高行　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内

⑦2発明者　秋山　良太　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内

⑦1出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地

⑦4代理人　弁理士　井桁　貞一

明　細　書

1. 発明の名称

暗号処理用鍵供給方式

2. 特許請求の範囲

【1】平文（P）と暗号文（C）との間の変換処理をDES方式に基づき実行する暗号化処理部（21）を具備し、相手装置（200）との間で暗号通信を実行する装置（100）において、

前記装置（100）外で生成された、前記暗号化処理部（21）が前記変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の暗号鍵（K_e）および復号鍵（K_d）の少なくも何れかを記憶し、前記暗号化処理部（21）に供給する鍵記憶手段（101）を設けることを特徴とする暗号処理用鍵供給方式。

【2】平文（P）と暗号文（C）との間の変換処理をDES方式に基づき実行する暗号化処理部（21）を具備し、相手装置（200）との間で暗号通信を実行する装置（100）において、

前記装置（100）外で生成された、前記暗号化処理部（21）が前記変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の暗号鍵（K_e）を記憶する暗号鍵記憶手段（102）と、

前記暗号鍵記憶手段（102）が記憶する前記暗号鍵（K_e）を抽出し、各十六段の順序を反転させて復号鍵（K_d）を生成し、前記暗号化処理部（21）に供給する反転処理手段（103）とを設けることを特徴とする暗号処理用鍵供給方式。

【3】平文（P）と暗号文（C）との間の変換処理をDES方式に基づき実行する暗号化処理部（21）を具備し、相手装置（200）との間で暗号通信を実行する装置（100）において、

前記装置（100）外で生成された、前記暗号化処理部（21）が前記変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分のマスタ鍵（K_m）を記憶するマスタ鍵記憶手段（105）と、

前記相手装置（200）と共用する48×16

ビットから成る同一の乱数を、共有するマスタ鍵（K_M）を用いてＤＥＳ方式に基づき暗号化処理し、それぞれ４８ビットから成る十六段分のセッション暗号鍵（K_{SS}）を生成する暗号処理手段（１０４）と、

前記暗号処理手段（１０４）が生成する前記セッション暗号鍵（K_{SS}）の、各十六段の順序を反転させてセッション復号鍵（K_{DS}）を生成し、前記暗号化処理部（２１）に供給する反転処理手段（１０３）とを設けることを特徴とする暗号処理用鍵供給方式。

【４】入力情報を暗号化処理部（２１）によりＤＥＳ方式に基づき暗号化処理し、暗号処理結果を相手装置（４００）との間で比較することにより相手装置（４００）を認証する装置（３００）において、

前記装置（３００）外で生成された、前記暗号化処理部（２１）が前記暗号処理を実行する為に必要とするそれぞれ４８ビットから成る十六段分の認証鍵（K_A）を記憶し、前記暗号化処理部（２１）に供給する認証鍵記憶手段（３０１）を設けることを特徴とする暗号処理用鍵供給方式。

【５】前記暗号鍵（K_S）、復号鍵（K_D）、マスタ鍵（K_M）および認証鍵（K_A）は、パリティビットを含む６４ビットから成るオリジナル鍵から、ＤＥＳ方式に基づき生成されることを特徴とする請求項１、２、３または４記載の暗号処理用鍵供給方式。

【６】前記暗号鍵（K_S）、復号鍵（K_D）、マスタ鍵（K_M）および認証鍵（K_A）は、パリティビットを含む６４ビットから成るオリジナル鍵から、前記ＤＥＳ方式に基づくこと無く生成されることを特徴とする請求項１、２、３または４記載の暗号処理用鍵供給方式。

3. 発明の詳細な説明

〔概要〕

ＤＥＳ方式に基づく暗号処理を採用する暗号通信システム、或いは認証システムにおける暗号処理用鍵供給方式に関し、

3

4

収容すべき手段を極力減少させることにより、収容手段量に制限のある装置においてもＤＥＳ方式に基づく暗号処理を適用可能とすることを目的とし、

平文と暗号文との間の変換処理をＤＥＳ方式に基づき実行する暗号化処理部を具備し、相手装置との間で暗号通信を実行する装置において、装置外で生成された、暗号化処理部が変換処理を実行する為に必要とするそれぞれ４８ビットから成る十六段分の暗号鍵および復号鍵の少なくも何れかを記憶し、暗号化処理部に供給する鍵記憶手段を設ける様に構成し、また装置外で生成された、暗号化処理部が変換処理を実行する為に必要とするそれぞれ４８ビットから成る十六段分の暗号鍵を記憶する鍵記憶手段と、鍵記憶手段が記憶する暗号鍵を抽出し、各十六段の順序を反転させて復号鍵を生成し、暗号化処理部に供給する反転処理手段とを設ける様に構成し、また装置外で生成された、暗号化処理部が変換処理を実行する為に必要とするそれぞれ４８ビットから成る十六段分のマスタ鍵を記憶するマスタ鍵記憶手段と、相手装置と共用する４８×１６ビットから成る同一の乱数を、共有するマスタ鍵を用いてＤＥＳ方式に基づき暗号化処理し、それぞれ４８ビットから成る十六段分のセッション暗号鍵を生成する暗号処理手段と、暗号処理手段が生成するセッション暗号鍵の、各十六段の順序を反転させてセッション復号鍵を生成し、暗号化処理部に供給する反転処理手段とを設ける様に構成し、また入力情報を暗号化処理部によりＤＥＳ方式に基づき暗号化処理し、暗号処理結果を相手装置との間で比較することにより相手装置を認証する装置において、装置外で生成された、暗号化処理部が暗号処理を実行する為に必要とするそれぞれ４８ビットから成る十六段分の認証鍵を記憶し、暗号化処理部に供給する認証鍵記憶手段を設ける様に構成し、なお暗号鍵、復号鍵、マスタ鍵および認証鍵は、パリティビットを含む６４ビットから成るオリジナル鍵から、ＤＥＳ方式に基づき生成される様に構成し、またＤＥＳ方式に基づくこと無く生成される様に構成

5

6

する。

〔産業上の利用分野〕

本発明は、ＤＥＳ方式に基づく暗号処理を採用する暗号通信システム、或いは認証システムにおける暗号処理用鍵供給方式に関する。

所要の情報を、第三者に秘匿して所定の相手との間で授受する暗号処理の一つとして、米国商務省により制定公布されたデータ暗号化規格（Data Encryption Standard、以後ＤＥＳと称する）が公知である。

一方、例えば銀行における窓口の無人化に伴い、顧客が所持するＩＣカードと銀行センタとの間で、第三者に秘匿すべき情報の授受、或いは情報授受相手の認証に、前述のＤＥＳ方式を採用する機会が増加しつつある。

〔従来の技術〕

第10図は従来ある暗号通信システムの一例を示す図であり、第11図は第10図における銀行センタ側装置の一例を示す図であり、第12図は第10図におけるＩＣカード側装置の一例を示す図である。

第10図において、銀行センタ１には、入力される平文ＰをＤＥＳ方式に基づき暗号文Ｃに変換する暗号化処理部１１と、銀行センタ１およびＩＣカード２が第三者に秘匿して保有する、パリティビットを含む６４ビットから成るオリジナル鍵Ｋ。から、暗号化処理部１１が暗号化を実行する為に必要とする、それぞれ４８ビットから成る十六段分の暗号鍵K_{E_1}～$K_{E_{16}}$を生成する鍵生成部１２とが設けられ、またＩＣカード２には、銀行センタ１から転送される暗号文Ｃを、ＤＥＳ方式に基づき平文Ｐに変換する暗号化処理部２１と、銀行センタ１およびＩＣカード２が第三者に秘匿して保有する、パリティビットを含む６４ビットから成るオリジナル鍵Ｋ。から、暗号化処理部２１が復号化を実行する為に必要とする、それぞれ４８ビットから成る十六段分の復号鍵Ｋ。を生成する鍵生成部２２とが設けられている。

第11図において、鍵生成部１２は、公知の如く、

オリジナル鍵Ｋ。を蓄積するレジスタＲＥＧ、第一縮約型転置部ＰＣ－１、十六段分の左シフタＳＦ－Ｌ、第二縮約型転置部ＰＣ－２および各種レジスタＲＥＧ類から構成され、オリジナル鍵Ｋ。から十六段分の暗号鍵K_{E_1}～$K_{E_{16}}$（各段の暗号鍵をそれぞれ第一段暗号鍵K_{E_1}乃至第十六段暗号鍵$K_{E_{16}}$と称する）を生成し、暗号化処理部１１の各段に供給する。

また暗号化処理部１１は、公知の如く、入力される平文Ｐを６４ビット宛蓄積するレジスタＲＥＧ、初期転置部ＩＰ、十六段分の暗号関数部ｆ、排他論理和部（＋）、レジスタＲＥＧ類、最終転置部IP^{-1}、出力される暗号文Ｃを６４ビット宛蓄積するレジスタＲＥＧから構成され、鍵生成部１２から各段の暗号関数部ｆにそれぞれ暗号鍵K_{E_1}乃至$K_{E_{16}}$を供給することにより、入力される平文Ｐを６４ビット宛、暗号文Ｃに変換して出力する。

一方第12図において、鍵生成部２２は、公知の如く、鍵生成部１２（第11図）における各左シフタＳＦ－Ｌを右シフタＳＦ－Ｒに変更することにより、オリジナル鍵Ｋ。から十六段分の復号鍵Ｋ。（各段の復号鍵をそれぞれ第一段復号鍵K_{D_1}乃至第十六段復号鍵$K_{D_{16}}$と称する）を生成し、暗号化処理部２１の各段に供給する。

また暗号化処理部２１は、公知の如く、入力される暗号文Ｃを６４ビット宛蓄積するレジスタＲＥＧ、初期転置部ＩＰ、十六段分の暗号関数部ｆ、排他論理和部（＋）、レジスタＲＥＧ類、最終転置部IP^{-1}、出力される平文Ｐを６４ビット宛蓄積するレジスタＲＥＧから構成され、鍵生成部２２から各段の暗号関数部ｆにそれぞれ復号鍵K_{D_1}乃至$K_{D_{16}}$を供給することにより、入力される暗号文Ｃを、平文Ｐに変換して出力する。

なおＤＥＳ方式においては、鍵生成部１２が暗号化処理部１１の各段に供給する第一段暗号鍵K_{E_1}乃至第十六段暗号鍵$K_{E_{16}}$と、鍵生成部２２が暗号化処理部２１の各段に供給する第一段復号鍵K_{D_1}乃至第十六段復号鍵$K_{D_{16}}$とを、$K_{E_1}=K_{D_{16}}$、$K_{E_2}=K_{D_{15}}$、……、$K_{E_{16}}=K_{D_1}$となる如

く生成することにより、暗号化処理部１１と２１とを同一構成としている。

次に第13図は従来ある認証システムの一例を示す図である。

第13図において、銀行センタ１には前述の暗号化処理部１１および鍵生成部１２の他に、乱数Ｒ₁を発生する乱数発生部１３と、比較部１４とが設けられており、またＩＣカード２には、前述と暗号化処理部２１と、銀行センタ１に設けられている鍵生成部１２と同一構成を有する鍵生成部２３とが設けられている。

銀行センタ１に設けられている鍵生成部１２と、ＩＣカード２に設けられている鍵生成部２３とは、それぞれ保有されている同一のオリジナル鍵Ｋ₀から、それぞれ４８ビットから成る十六段分の認証鍵Ｋ$_{a}$を生成し、それぞれ暗号化処理部１１および２１の各段に供給する。

一方銀行センタ１に設けられている乱数発生部１３は、乱数Ｒ₁を発生して暗号化処理部１１に入力すると共に、ＩＣカード２にも転送し、暗号化処理部２１に入力する。

各暗号化処理部１１および２１は、それぞれ鍵生成部１２および２３から認証鍵Ｋ$_{a}$を供給されることにより、入力される乱数Ｒ₁を、それぞれ暗号化乱数Ｒ$_{c1}$およびＲ$_{c2}$に変換し、銀行センタ１に設けられた比較部１４に伝達する。

比較部１４は、暗号化処理部１１から伝達される暗号化乱数Ｒ$_{c1}$と、暗号化処理部２１から伝達される暗号化乱数Ｒ$_{c2}$とを比較し、両者が一致した場合には、銀行センタ１はＩＣカード２を認証する。

〔発明が解決しようとする課題〕

以上の説明から明らかな如く、従来ある暗号通信システムにおいては、ＩＣカード２に鍵生成部２２を設ける必要があり、また従来ある認証システムにおいても、ＩＣカード２に鍵生成部２３を設ける必要があり、ＩＣカード２に収容し切れぬ問題があった。

本発明は、収容すべき手段を極力減少させることにより、収容手段量に制限のある装置においてもＤＥＳ方式に基づく暗号処理を適用可能とすることを目的とする。

〔課題を解決するための手段〕

第１図は本発明の原理を示す図であり、同図（ａ）は請求項１に関する原理を示し、同図（ｂ）は請求項２に関する原理を示し、同図（ｃ）は請求項３に関する原理を示し、同図（ｄ）は請求項４に関する原理を示す。

第１図において、１００は暗号通信を行う装置、２００は装置１００との間の暗号通信の相手装置、３００は認証を行う装置、４００は装置３００との認証の相手装置、１１は相手装置２００が具備する暗号化処理部、２１は装置１００および３００が具備する暗号化処理部である。

１０１は、本発明（請求項１）により装置１００に設けられた鍵記憶手段である。

１０２は、本発明（請求項２）により装置１００に設けられた暗号鍵記憶手段である。

１０３は、本発明（請求項２および請求項３）により装置１００に設けられた反転処理手段である。

１０４は、本発明（請求項３）により装置１００に設けられた暗号処理手段である。

１０５は、本発明（請求項３）により装置１００に設けられたマスタ鍵記憶手段である。

３０１は、本発明（請求項４）により装置３００に設けられた認証鍵記憶手段３０１である。

〔作用〕

暗号化処理部２１は、平文Ｐと暗号文Ｃとの間の変換処理をＤＥＳ方式に基づき実行する。

鍵記憶手段１０１は、装置１００外で生成された、暗号化処理部２１が変換処理を実行する為に必要とする、それぞれ４８ビットから成る十六段分の暗号鍵Ｋ$_{a}$および復号鍵Ｋ$_{b}$の少なくも何れかを記憶し、暗号化処理部２１に供給する。

暗号鍵記憶手段１０２は、装置１００外で生成された、暗号化処理部２１が変換処理を実行する

為に必要とする、それぞれ４８ビットから成る十六段分の暗号鍵K_sを記憶する。

反転処理手段１０３は、暗号鍵記憶手段１０２が記憶する暗号鍵K_sを抽出し、各十六段の順序を反転させて復号鍵K_oを生成し、暗号化処理部２１に供給する。

マスタ鍵記憶手段１０５は、装置１００外で生成された、暗号化処理部２１が変換処理を実行する為に必要とする、それぞれ４８ビットから成る十六段分のマスタ鍵K_mを記憶する。

暗号処理手段１０４は、相手装置２００と共用する４８×１６ビットから成る同一の乱数を、共有するマスタ鍵K_mを用いてＤＥＳ方式に基づき暗号化処理し、それぞれ４８ビットから成る十六段分のセッション暗号鍵K_{ss}を生成する。

認証鍵記憶手段３０１は、装置３００外で生成された、暗号化処理部２１が暗号処理を実行する為に必要とする、それぞれ４８ビットから成る十六段分の認証鍵K_Aを記憶し、暗号化処理部２１に供給する。

なお暗号鍵K_s、復号鍵K_o、マスタ鍵K_mおよび認証鍵K_Aは、パリティビットを含む６４ビットから成るオリジナル鍵から、ＤＥＳ方式に基づき生成されることが考慮される。

また暗号鍵K_s、復号鍵K_o、マスタ鍵K_mおよび認証鍵K_Aは、パリティビットを含む６４ビットから成るオリジナル鍵から、ＤＥＳ方式に基づくこと無く生成されることが考慮される。

従って、本発明（請求項１乃至請求項６）によれば、装置にはＤＥＳ方式に基づく暗号処理に必要とする鍵生成部を設ける必要が無くなり、装置の小形化、軽量化および経済化を大幅に向上する。

〔実施例〕

以下、本発明の一実施例を図面により説明する。第２図は本発明（請求項１および請求項５）の一実施例による暗号通信システムを示す図であり、第３図は本発明（請求項２および請求項５）の一実施例による暗号通信システムを示す図であり、第４図は第３図における反転処理部の一例を示す

図であり、第５図は第３図に対応する双方向暗号通信システムを示す図であり、第６図は本発明（請求項２および請求項６）の一実施例による暗号通信システムを示す図であり、第７図は本発明（請求項３および請求項５）の一実施例による暗号通信システムを示す図であり、第８図は本発明（請求項４および請求項５）の一実施例による認証システムを示す図であり、第９図は本発明（請求項４および請求項６）の一実施例による認証システムを示す図である。なお、全図を通じて同一符号は同一対象物を示す。また装置１００は何れもＩＣカード２とし、相手装置２００は何れも銀行センタ１とする。

第２図においては、第１図（ａ）における鍵記憶手段１０１として鍵レジスタ２４が設けられ、また第３図においては、第１図（ｂ）における暗号鍵記憶手段１０２として鍵レジスタ２５が設けられ、また第１図（ｂ）における反転処理手段１０３として反転処理部２６が設けられ、また第６図においては、第１図（ｂ）における暗号鍵記憶手段１０２として鍵レジスタ２７が設けられ、また第１図（ｂ）における反転処理手段１０３として反転処理部２６が設けられ、また第７図においては、第１図（ｃ）における暗号鍵記憶手段１０２として鍵レジスタ４４が設けられ、また第１図（ｃ）における暗号処理手段１０４として暗号化処理部２１が使用され、また第１図（ｃ）における反転処理手段１０３として反転処理部４５が設けられ、また第８図においては、第１図（ｄ）における認証鍵記憶手段３０１として鍵レジスタ２５が設けられ、また第９図においては、第１図（ｄ）における認証鍵記憶手段３０１として鍵レジスタ２７が設けられている。

最初に、第２図乃至第７図に基づき本発明の一実施例による暗号通信システムを説明する。

第２図において、銀行センタ１には、前述（第10図）と同様の暗号化処理部１１および鍵生成部１２が設けられており、鍵生成部１２は、パリティビットを含む６４ビットから成るオリジナル鍵K_oから、それぞれ４８ビットから成る十六段分

の暗号鍵K_Eおよび復号鍵K_Dを生成する。

一方ＩＣカード２には、第10図における鍵生成部２２の代わりに鍵レジスタ２４が設けられ、銀行センタ１において鍵生成部１２が生成する復号鍵K_Dが蓄積されている。

銀行センタ１においては、前述（第10図）と同様の過程で、暗号化処理部１１が鍵生成部１２から暗号鍵K_Eを供給されることにより、入力される平文Ｐを暗号文Ｃに変換し、ＩＣカード２に転送する。

ＩＣカード２における暗号化処理部２１は、鍵レジスタ２４に蓄積済の復号鍵K_Dを供給されることにより、前述（第10図）と同様の過程で、銀行センタ１から転送される暗号文Ｃを平文Ｐに変換し、出力する。

次に第３図において、銀行センタ１には、前述（第10図）と同様に暗号化処理部１１および鍵生成部１２が設けられており、鍵生成部１２は、前述（第10図）と同様に、オリジナル鍵K_Oから暗号鍵K_Eを生成して暗号化処理部１１に供給し、

した復号鍵K_Dを供給されることにより、暗号化処理部１１と同一構成を有し、暗号化処理部１１から転送された暗号文Ｃを平文Ｐに変換する。

第５図は、第３図における銀行センタ１に反転処理部１８およびセレクタ１９を追加し、またＩＣカード２にセレクタ２８を追加することにより、銀行センタ１とＩＣカード２との間の双方向暗号通信を可能としたものである。

第５図においては、銀行センタ１のセレクタ１９および第２図のセレクタ２８をそれぞれ「Ａ」側に設定することにより、第３図におけると同様に、銀行センタ１の暗号化処理部１１が鍵生成部１２から暗号鍵K_Eを供給されて平文Ｐを暗号文Ｃに変換してＩＣカード２に転送し、ＩＣカード２の暗号化処理部２１が反転処理部２６から復号鍵K_Dを供給されて暗号文Ｃを平文Ｐに変換して出力するが、銀行センタ１のセレクタ１９およびＩＣカード２のセレクタ２８をそれぞれ「Ｂ」側に設定することにより、第３図におけると逆に、ＩＣカード２の暗号化処理部２１が鍵レジスタ２

暗号化処理部１１は、前述（第２図）と同様に、鍵生成部１２から暗号鍵K_Eを供給されることにより、入力される平文Ｐを暗号文Ｃに変換し、ＩＣカード２に転送する。

一方ＩＣカード２には、第10図における鍵生成部２２の代わりに鍵レジスタ２５および反転処理部２６が設けられ、鍵レジスタ２５には、銀行センタ１において鍵生成部１２が生成する暗号鍵K_Eが蓄積されている。

反転処理部２６は、第４図に示される如く、鍵レジスタ２５に蓄積済の暗号鍵K_Eを抽出し、第一段暗号鍵K_{E1}を第十六段復号鍵K_{D16}、第二段暗号鍵K_{E2}を第十五段復号鍵K_{D15}、以下同様にして、第十五段暗号鍵K_{E15}を第二段復号鍵K_{D2}、第十六段暗号鍵K_{E16}を第一段復号鍵K_{D1}に、それぞれ各段の順序を反転して暗号鍵K_Eから復号鍵K_Dを生成し、暗号化処理部２１に供給する。

暗号化処理部２１は、前述（第11図および第12図）の如く、銀行センタ１において暗号化処理部１１が供給された暗号鍵K_Eの各段の順序を反転

５から暗号鍵K_Eを供給されて平文Ｐを暗号文Ｃに変換して銀行センタ１に転送し、銀行センタ１の暗号化処理部１１が反転処理部１８から復号鍵K_Dを供給されて暗号文Ｃを平文Ｐに変換して出力する。

次に第６図においては、銀行センタ１において、第３図における鍵生成部１２の代わりに、乱数発生部１６および鍵レジスタ１７が設けられており、またＩＣカード２において、第３図における鍵レジスタ２５の代わりに鍵レジスタ２７が設けられている。

銀行センタ１において、乱数発生部１６は、４８×１６（＝７６８）ビットの乱数を暗号鍵K_{EE}として発生し、鍵レジスタ１７は、乱数発生部１６が発生した暗号鍵K_{EE}を蓄積し、暗号化処理部１１に供給する。

ＩＣカード２において、鍵レジスタ２７には、銀行センタ１において鍵レジスタ１７が蓄積する暗号鍵K_{EE}が蓄積されている。

銀行センタ１においては、暗号化処理部１１が、

鍵レジスタ１７に蓄積済の暗号鍵K_{ss}を供給されることにより、入力される平文Ｐを暗号文Ｃに変換し、ＩＣカード２に転送する。

ＩＣカード２においては、反転処理部２６が、前述（第３図）と同様に、鍵レジスタ２７に蓄積済の暗号鍵K_{ss}を抽出し、それぞれ各段の順序を反転して復号鍵K_{ds}を生成し、暗号化処理部２１に供給する。

暗号化処理部２１は、前述（第３図）と同様に、反転処理部２６から復号鍵K_{ds}を供給されることにより、暗号化処理部１１から転送された暗号文Ｃを、平文Ｐに変換する。

次に第７図においては、銀行センタ１には第３図における暗号化処理部１１および鍵生成部１２の他に、セレクタ３１乃至３３と、乱数発生部３４と、鍵レジスタ３５とが設けられ、またＩＣカード２には第３図における暗号化処理部２１、鍵レジスタ２５および反転処理部２６の他に、セレクタ４１乃至４３および鍵レジスタ４４が設けられている。

当初、銀行センタ１におけるセレクタ３１乃至３３、およびＩＣカード２におけるセレクタ４１乃至４３は、何れも「Ａ」側に設定されている。

その結果、銀行センタ１においては、鍵生成部１２がマスタ鍵K_mから生成した暗号鍵K_sが、セレクタ３３を介して暗号化処理部１１に供給されており、またＩＣカード２においては、鍵レジスタ２５に蓄積されている暗号鍵K_sがセレクタ４３を介して暗号化処理部２１に供給されている。

かかる状態で、乱数発生部３４は、各セッション毎にそれぞれ４８×１６（＝７６８）ビットから成るセッション乱数R_sを発生し、セレクタ３１を介して暗号化処理部１１に入力すると共に、ＩＣカード２にも転送し、セレクタ４１を介して暗号化処理部１１と同一構成を有する暗号化処理部２１に入力する。

暗号鍵K_sを供給されている暗号化処理部１１は、入力されたセッション乱数R_sを暗号化してセッション暗号鍵K_{ss}を生成し、セレクタ３２を介して鍵レジスタ３５に蓄積する。

また暗号鍵K_sを供給されている暗号化処理部２１も、入力されたセッション乱数R_sを暗号化し、暗号化処理部１１が生成したと同一のセッション暗号鍵K_{ss}を生成し、セレクタ４２を介して鍵レジスタ４４に蓄積する。

反転処理部２６は、前述（第３図）と同様に、鍵レジスタ４４に蓄積されているセッション暗号鍵K_{ss}を抽出し、それぞれ各段の順序を反転してセッション復号鍵K_{ds}を生成し、セレクタ４３の「Ｂ」側に供給する。

かかる状態で、銀行センタ１におけるセレクタ３１乃至３３、およびＩＣカード２におけるセレクタ４１乃至４３を、それぞれ「Ｂ」側に切替えると、銀行センタ１においては、暗号化処理部１１が、鍵レジスタ３５に蓄積されているセッション暗号鍵K_{ss}をセレクタ３３を介して供給されることにより、該セッションにおいて入力される平文P_sを暗号文C_sに変換し、セレクタ３２を介してＩＣカード２に転送する。

ＩＣカード２においては、暗号化処理部２１が、反転処理部２６からセレクタ４３を介してセッション復号鍵K_{ds}を供給されることにより、銀行センタ１からセレクタ４１を介して転送される暗号文C_sを平文P_sに変換し、セレクタ４２を介して出力する。

以上により、銀行センタ１とＩＣカード２との間では、各セッション毎に異なるセッション乱数R_sから暗号化処理部１１と、暗号化処理部２１および反転処理部２６とにより暗号化されて生成されたセッション暗号鍵K_{ss}およびセッション復号鍵K_{ds}を用いて暗号通信が実行される。

次に、第８図および第９図に基づき本発明の一実施例による認証システムを説明する。

第８図において、銀行センタ１には前述（第13図）と同様に、暗号化処理部１１、鍵生成部１２、乱数発生部１３および比較部１４が設けられているが、ＩＣカード２には鍵生成部２３の代わりに鍵レジスタ２５が設けられている。

鍵レジスタ２５には、銀行センタ１において鍵生成部１２がオリジナル鍵K_oから生成する認証

鍵K_Aが蓄積されており、暗号化処理部２１の各段に供給されている。

かかる状態で、銀行センタ１に設けられている乱数発生部１３は、前述（第13図）と同様に、乱数R_1を発生して暗号化処理部１１に入力すると共に、ＩＣカード２にも転送し、暗号化処理部２１に入力する。

各暗号化処理部１１および２１は、前述（第13図）と同様に、それぞれ鍵生成部１２および鍵レジスタ２５から認証鍵K_Aを供給されることにより、入力される乱数R_1をそれぞれ暗号化乱数R_{c1}およびR_{c2}に変換し、銀行センタ１に設けられた比較部１４に伝達する。

比較部１４は、暗号化処理部１１から伝達される暗号化乱数R_{c1}と、暗号化処理部２１から伝達される暗号化乱数R_{c2}とを比較し、両者が一致した場合には、銀行センタ１はＩＣカード２を認証する。

次に第９図において、銀行センタ１には、第８図における鍵生成部１２の代わりに、乱数発生部１６および鍵レジスタ１７が設けられており、またＩＣカード２には、第８図における鍵レジスタ２５の代わりに鍵レジスタ２７が設けられている。

銀行センタ１において、乱数発生部１６は、４８×１６（＝７６８）ビットの乱数を認証鍵K_{AR}として発生し、鍵レジスタ１７は、乱数発生部１６が発生した認証鍵K_{AR}を蓄積し、暗号化処理部１１に供給する。

ＩＣカード２において、鍵レジスタ２７には、銀行センタ１において鍵レジスタ１７が蓄積する認証鍵K_{AR}が蓄積され、暗号化処理部２１の各段に供給している。

かかる状態で、銀行センタ１に設けられている乱数発生部１３は、前述（第８図）と同様に、乱数R_1を発生して暗号化処理部１１に入力すると共に、ＩＣカード２にも転送し、暗号化処理部２１に入力する。

各暗号化処理部１１およひ２１は、前述（第８図）と同様に、それぞれ鍵レジスタ１７および２７から認証鍵K_{AR}を供給されることにより、入力

される乱数R_1をそれぞれ暗号化乱数R_{c1}およびR_{c2}に変換し、銀行センタ１に設けられた比較部１４に伝達する。

比較部１４は、暗号化処理部１１から伝達される暗号化乱数R_{c1}と、暗号化処理部２１から伝達される暗号化乱数R_{c2}とを比較し、両者が一致した場合には、銀行センタ１はＩＣカード２を認証する。

以上の説明から明らかな如く、本実施例によれば、ＩＣカード２には鍵生成部２２を設ける代わりに、銀行センタ１で生成された復号鍵K_Dを蓄積する鍵レジスタ２４を設けるか、或いは銀行センタ１で生成された暗号鍵K_E、K_{SE}またはセッション暗号鍵K_{SS}を蓄積する鍵レジスタ２５、２７または４４と、反転処理部２６とを設けることにより、暗号化処理部２１が暗号文Ｃを平文Ｐに変換することが可能となり、所要の暗号通信が実現可能となり、またＩＣカード２に鍵生成部２３を設ける代わりに、銀行センタ１で生成された認証鍵K_AまたはK_{AR}を蓄積する鍵レジスタ２５または２７を設けにことにより、暗号化処理部２１が乱数R_1を暗号化乱数R_{c2}に変換可能となり、所要の認証が可能となる。

なお、第２図乃至第９図はあく迄本発明の一実施例に過ぎず、例えば第２図における暗号鍵K_Eはオリジナル鍵K_Oから鍵生成部１２および鍵生成部１５により生成されるものに限定されることは無く、乱数発生部１６および反転処理部１８により生成する等、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。また第２図、第６図および第７図に示される暗号通信システムは、一方向通信のみに限定されることは無く、第３図に対する第５図の如く、双方向通信とすることも考慮されるが、かかる場合にも本発明の効果は変わらない。また第８図および第９図に示される認証システムは、銀行センタ１からＩＣカード２を一方向認証するものに限定されることは無く、ＩＣカード２から銀行センタ１の認証、更には双方向認証とすることも考慮されるが、かかる場合にも本発明の効果は変わらない。更に本

発明の対象とする装置１００、３００および相手装置２００、４００は、ＩＣカード２と銀行センタ１とに限定されぬことは言う迄も無い。

〔発明の効果〕

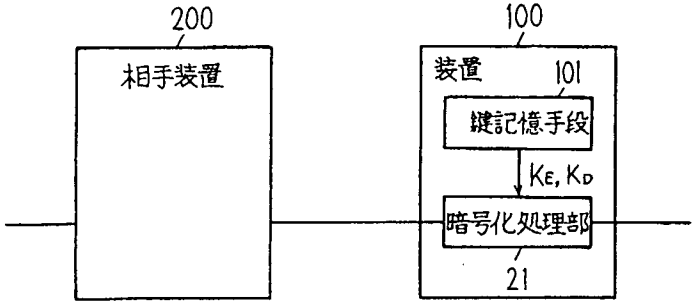
以上、本発明（請求項１乃至請求項６）によれば、装置にはＤＥＳ方式に基づく暗号処理に必要とする鍵生成部を設ける必要が無くなり、装置の小形化、軽量化および経済化を大幅に向上する。

4. 図面の簡単な説明

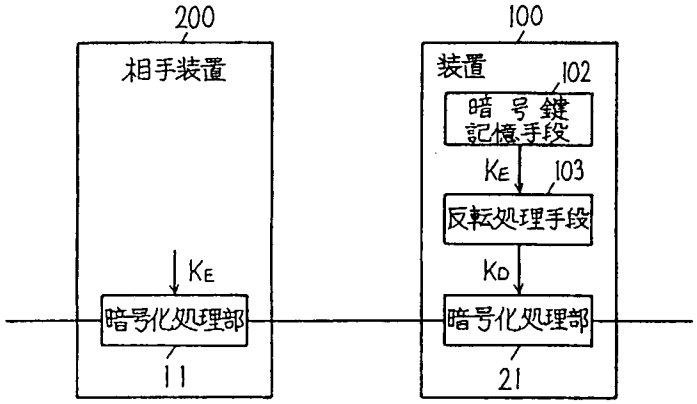
第１図は本発明の原理を示す図で、同図（ａ）は請求項１に関する原理を示し、同図（ｂ）は請求項２に関する原理を示し、同図（ｃ）は請求項３に関する原理を示し、同図（ｄ）は請求項４に関する原理を示し、第２図は本発明（請求項１および請求項５）の一実施例による暗号通信システムを示す図、第３図は本発明（請求項２および請求項５）の一実施例による暗号通信システムを示す図、第４図は第３図における反転処理部の一例を示す図、第５図は第３図に対応する双方向暗号通信システムを示す図、第６図は本発明（請求項２および請求項６）の一実施例による暗号通信システムを示す図、第７図は本発明（請求項３および請求項５）の一実施例による暗号通信システムを示す図、第８図は本発明（請求項４および請求項５）の一実施例による認証システムを示す図、第９図は本発明（請求項４および請求項６）の一実施例による認証システムを示す図、第10図は従来ある暗号通信システムの一例を示す図、第11図は第10図における銀行センタ側装置の一例を示す図、第12図は第10図におけるＩＣカード側装置の一例を示す図、第13図は従来ある認証システムの一例を示す図である。

図において、１は銀行センタ、２はＩＣカード、１１および２１は暗号化処理部、１２、２２および２３は鍵生成部、１３、１６および３４は乱数発生部、１４は比較部、１７、２４、２５、２７、３５および４４は鍵レジスタ、１８および２６は反転処理部、１９、２８、３１乃至３３および４１乃至４３はセレクタ、１００および３００は装置、２００および４００は相手装置、１０１は鍵記憶手段、１０２は暗号鍵記憶手段、１０３は反転処理手段、１０４は暗号処理手段、１０５はマスタ鍵記憶手段、３０１は認証鍵記憶手段、を示す。

代理人　弁理士　井　桁　貞　一

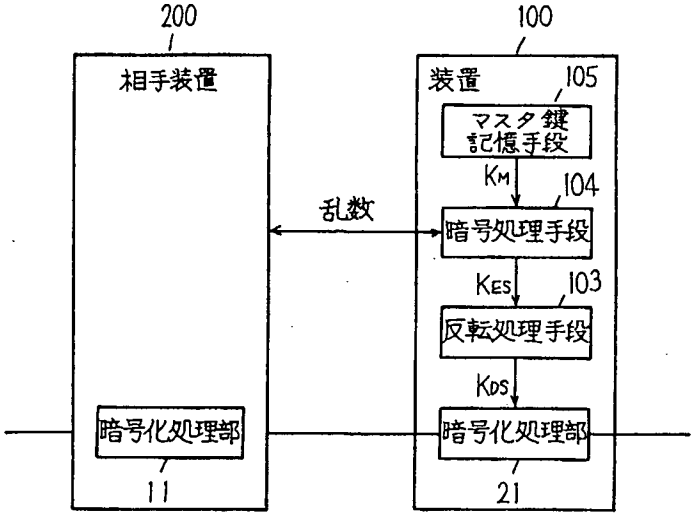


(a) 本発明(請求項1)の原理図

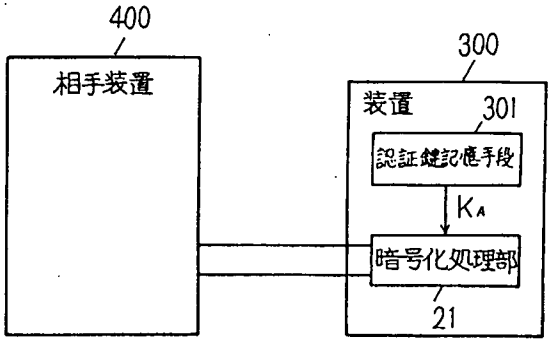


(b) 本発明(請求項2)の原理図

本発明の原理図
第1図(その1)

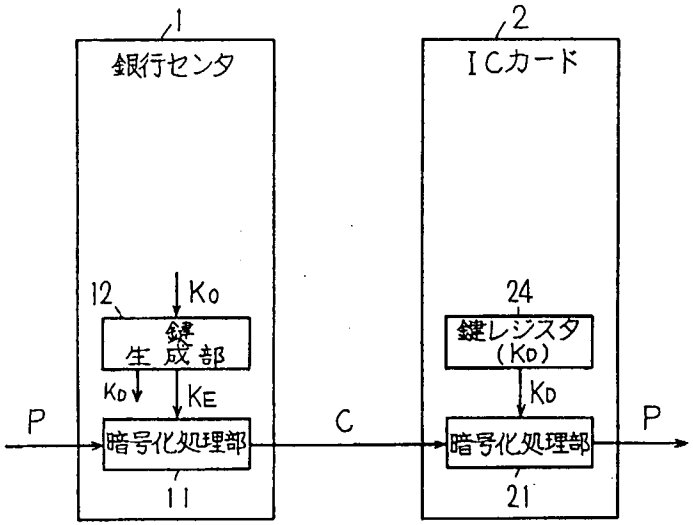


(C) 本発明(請求項3)の原理図



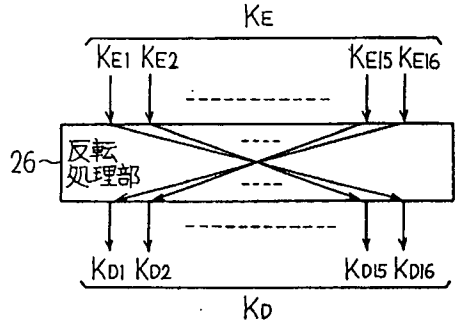
(d) 本発明(請求項4)の原理図

本発明の原理図
第1図(その2)



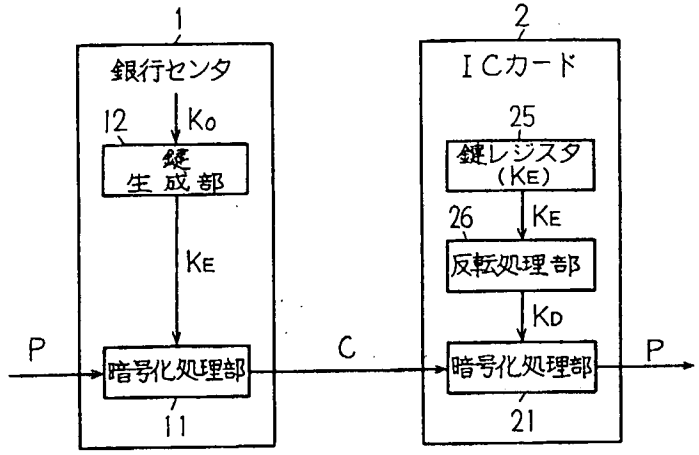
本発明(請求項1および請求項5)による暗号通信システム

第 2 図



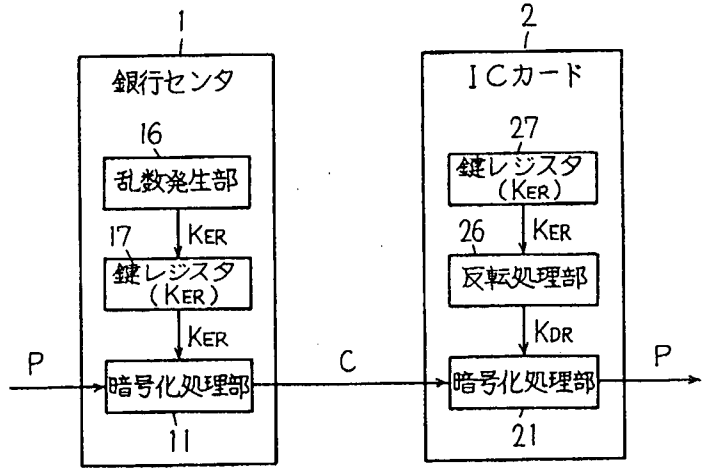
第3図における反転処理部

第 4 図



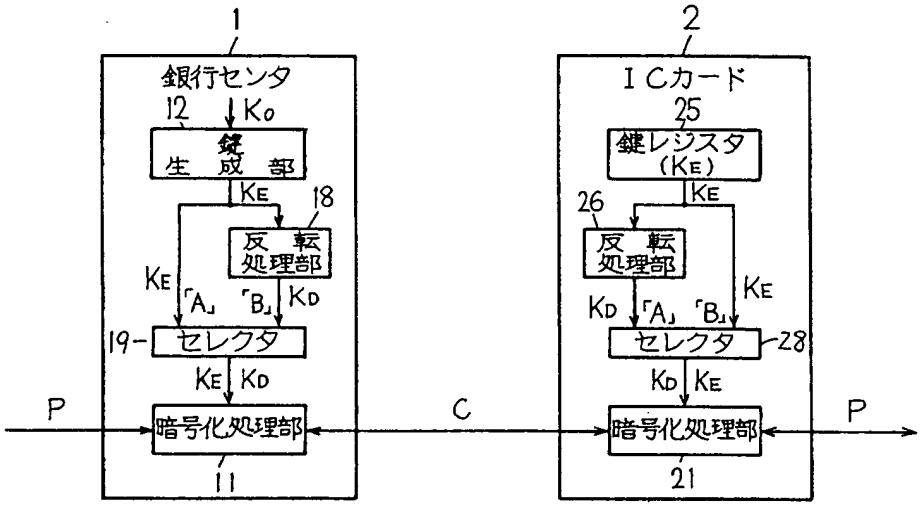
本発明(請求項2および請求項5)による暗号通信システム

第 3 図



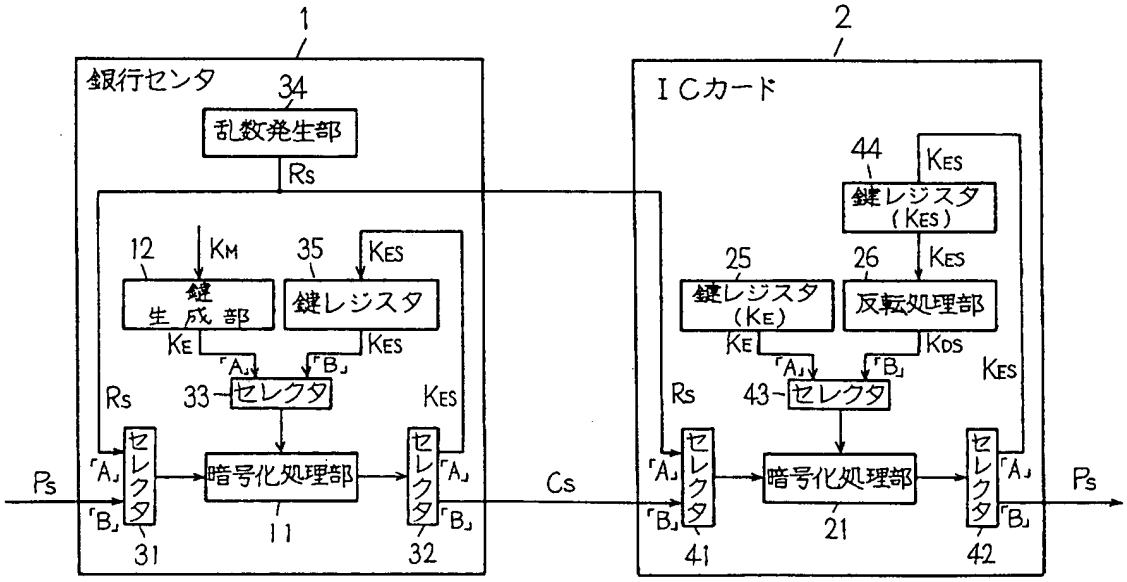
本発明(請求項2および請求項6)による暗号通信システム

第 6 図



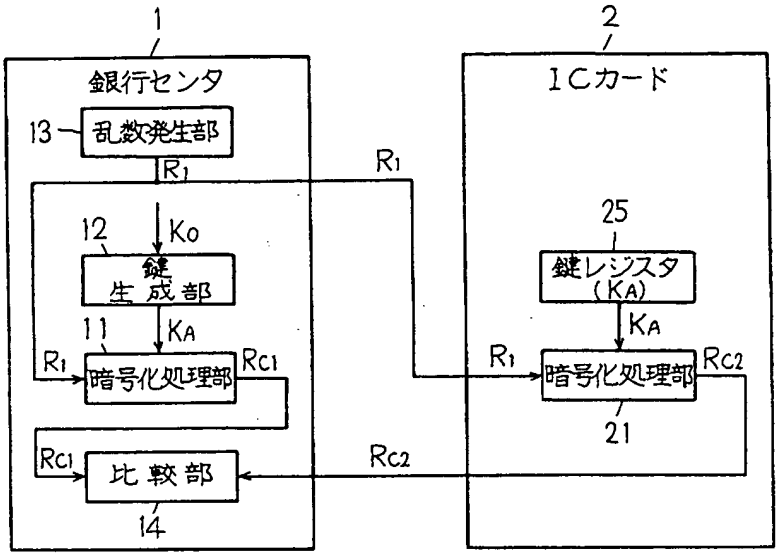
第3図に対応する双方向暗号通信システム

第 5 図



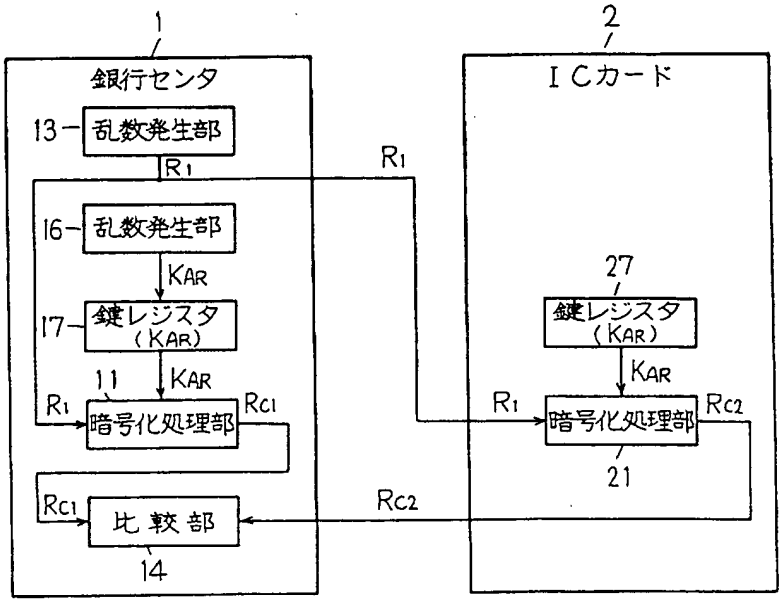
本発明（請求項3および請求項5）による暗号通信システム

第 7 図



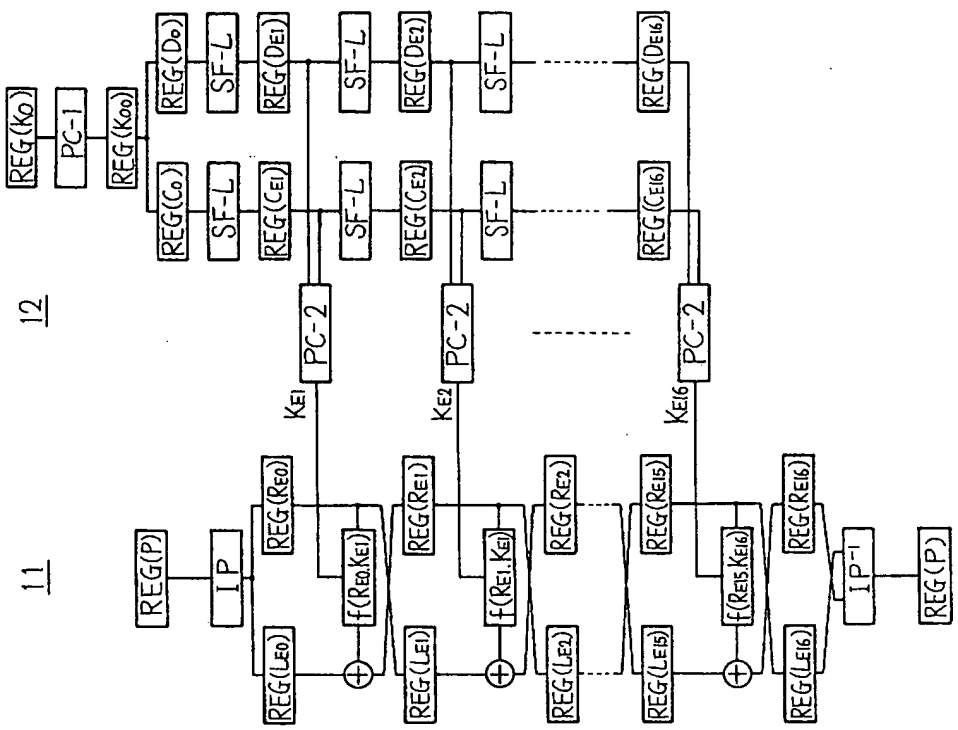
本発明（請求項4および請求項5）による認証システム

第 8 図



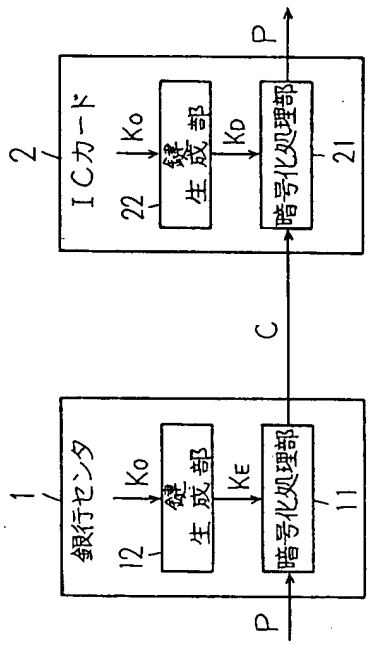
本発明（請求項4および請求項6）による認証システム

第 9 図



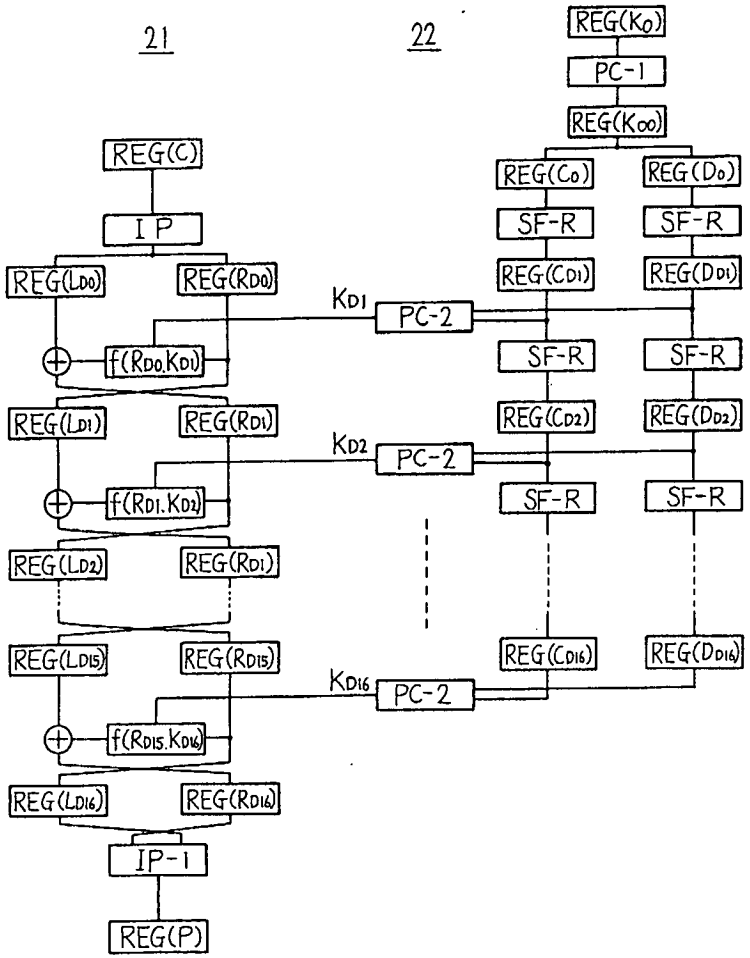
第10図における銀行センタ側装置

第 11 図



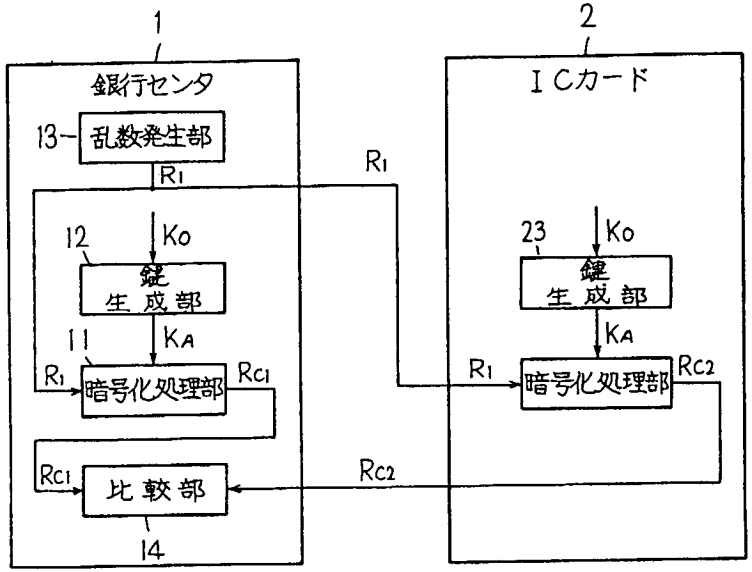
従来ある暗号通信システム

第 10 図



第10図におけるICカード側装置

第 12 図



従来ある認証システム

第 13 図